Amendments to the Claims:

This listing of claims will replace all prior versions,
and listings, of claims in the application:

Listing of Claims:

Claim 1 (original):   A   system   for   generating
and ordering an identification document over a network,
the system comprising:

a   user   interface   connected   to   the   network 'in
communication with a server also coupled to the network;

a   data   gathering   module   coupled   to   said   server,
said data gathering module capable of prompting a user
to   provide   at   least   one   demographic   data   and   a
corresponding graphical representation and receiving and
securely storing said at least one demographic data and
said   corresponding   graphical   representation   in   a   user
demographic and picture data database coupled to said
server;

an identification document design module coupled to
said   server,   said   design   module   capable   of   providing
identification   document   design   guidance   data   to   said
user   and   thereby   prompting   said   user   to   provide
identification document design data, the design module
capable of receiving and securely storing identification
document   design   data   in   a   document   design   data   base
coupled to said server;

a payment module coupled to said server, said payment module capable of prompting the user to provide payment data and receiving and securely storing said payment data in said user database, said payment data including user location data and user payment data, said payment data being utilized to verify that a payment for said identification document has been made and to provide a paid-in-full signal upon said verification;

a user verification module coupled to said server, said user verification module capable of retrieving said user location data, authenticating the identity of said user, and providing a user verification signal upon successful user authentication;

a service bureau coupled to said server and responsive to said paid-in-full signal, whereby in response to said paid-in-full signal and said user verification signal, said service bureau retrieves from said user data base said at least one demographic data and said corresponding graphical representation and retrieves from said document design data base said identification document design data, and produces a draft identification document incorporating said at least one demographic data and said corresponding graphical representation and said identification document design data;

a user approval module coupled to said server, said user approval module capable of providing a facsimile of said draft identification document to the user over said

server through said network, and prompting the user to provide a job-acceptance signal;

said service bureau providing a final identification document to said user in response to said job-acceptance signal, said final identification document being the equivalent of an approved said draft identification document.

Claim 2 (original): The system as in claim 1, wherein said data gathering module, said identification document design module, said payment module, said service bureau, said user approval module and said user verification module, can be coupled to said server by one of the following group consisting of an Internet network connection, an intranet network connection, a dial-up modem connection, and further wherein each module includes a plurality of computer processor instructions that can be executed by a computer processor located within said server and at least one processor remote from said server, wherein said computer processor instructions can be compiled instructions written in one of the group of computer languages consisting of C, C++, and Java and can be interpreted instructions written in one of the following group of computer languages consisting of visual basic, Java script, CGI script.

Claim 3 (original): The system as in claim 1, wherein said at least one demographic data includes: the name of an employee, the name of a company, the employee number, the address of a company, the telephone number of a company, a security clearance level.

Claim 4 (original): The system as in claim 1, wherein said corresponding graphical representation can include a digitally encoded picture, and a digitally encoded fingerprint.

Claim 5 (original): The system as in claim 1, wherein said securely storing said at least one demographic data and said corresponding graphical representation includes encrypting said at least one demographic data and said corresponding graphical representation using a password to generate a plurality of password encrypted data.

Claim 6 (original): The system as in claim 1, wherein said identification document design guidance data includes: a plurality of identification document orientation data including portrait and landscape orientations; a plurality of location data for placement of said graphical representation; a plurality of location data, orientation data, font type data, font size data for placement of said at least one demographic data on said identification document; a plurality of

special printable indicia of security clearance level data; and a plurality of data for printing on both sides of said identification document.

Claim 7 (original): The system as in claim 1, wherein said payment data includes: a shipping address; credit card information necessary to effectuate a credit purchase; debit card information necessary to effectuate a debit purchase; electronic transfer authorization information necessary to effectuate a credit purchase; and a purchase order number.

Claim 8 (original): The system as in claim 1, wherein said user verification module includes a database containing a plurality of business addresses and corresponding telephone numbers, wherein said location of the user is cross-checked with said business address and telephone numbers in said data base.

Claim 9 (original): The system as in claim 1, further comprising:

a security feature design module configured and arranged to provide the user with security feature design guidance data and to prompt the user to provide security feature design data, said security feature design wizard securely storing said security feature design data in a user security feature database wherein said security feature design guidance data includes data

directed to: an encoded magnetic stripe; a one-dimensional bar code; a two-dimensional bar code; micro-printing one or more characters; one or more UV visible security features printed on said document; and to securely store said security feature design data in a password encrypted file.

Claim 10 (original): The system as in claim 1, further comprising a user registration module coupled to said server configured and arranged to query the user to provide at least one user data, and configured and arranged to receive said at least one user data and to securely store said at least one user data; wherein said at least one user data includes: a name of the user; a name of a company associated with the user; a location of said company associated with the user; a telephone number associated with the user; an e-mail address associated with the user.

Claim 11 (currently amended): A method for a user to order customized identification documents over a network connected to a user interface in communication with a server coupled to the network, the method comprising the steps of:

providing the user with a plurality of badge design guidance data;

receiving a plurality of design badge data from the user;

storing said plurality of design badge data;

prompting the user to provide at least one demographic data to be incorporated into said identification document;

receiving said at least one demographic data to be incorporated into said identification document

prompting the user to provide at least one graphical representation corresponding to said at least one demographic data to be incorporated into said identification document;

receiving at least one graphical representation corresponding to said at least one demographic data to be incorporated into said identification document;

securely storing said at least one demographic data and corresponding at least one graphical representation;

creating at least one facsimile of an identification document incorporating said plurality of design badge data and including said at least one demographic data and corresponding at least one graphical representation;

providing said at least one facsimile to the user;

prompting the user to approve or not approve the facsimile;

receiving the approval or not approval from the user;

if approval is received and then no payment data is stored then prompt the user for payment and location

information, otherwise retrieve stored payment data including said location information;

if approval is received and no payment data is stored then receive said payment and location information;

if approval is received then verify that said location information is a legitimate organization;

if approval is received then verify using said payment information that a payment has been received;

if approval is received and the location information is verified, and if a verified payment has been received then manufacture said at least one identification document corresponding to the approved at least one facsimile;

deliver to said location said at least one identification document to the user.

Claim 12 (original): The method as in claim 11, further comprising the steps of:

providing the user with a user id and password;

prompting the user to provide at least one user data;

receiving said at least one user data; and

securely storing said at least one user data.

Claim 13 (original): The method of claim 11, wherein the step of verifying that said location is a legitimate organization includes:

retrieving said location information;

cross checking said location information with a database of known legitimate organizations.

Claim 14 (original): The method of claim 11, further comprising the steps of:

providing the user with a plurality of security feature design guidance data;

receiving from the user a plurality of security feature design data;

securely storing said security feature design data in a security feature design data database.